

Cloudflare Area 1 y Google Cloud:

Seguridad integrada del correo electrónico en la nube y protección preventiva contra phishing

Desafíos de la industria:

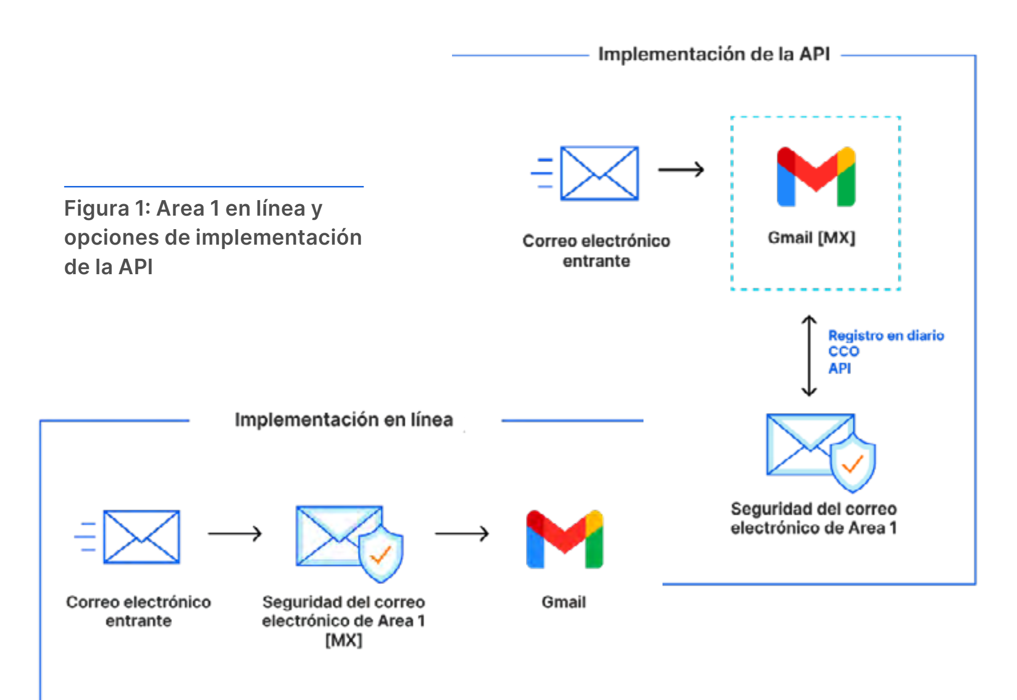
Hoy en día, los sofisticados ataques de phishing como, por ejemplo, los ataques al correo electrónico corporativo (BEC) sin malware, el fraude basado en la apropiación de cuentas y las amenazas internas son difíciles de detectar para las puertas de enlace de correo electrónico seguras o los métodos de autenticación del correo electrónico tradicionales.

La solución:

El servicio de seguridad del correo electrónico de Cloudflare Area 1 rastrea proactivamente la web en busca de campañas de phishing y utiliza esta información inicial, junto con las técnicas de análisis contextual del correo electrónico, para proteger tus buzones contra los ataques de phishing, antes de que estos puedan causar daños.

Basado en Google Cloud Platform, Area 1 se implementa en solo unos minutos, y proporciona la mejor capa de seguridad de protección integral contra phishing.

Figura 1: Area 1 en línea y opciones de implementación de la API



Protégete de los ataques modernos contra tu aplicación más importante en la nube: el correo electrónico.



Detén de forma preventiva el phishing, los ataques al correo electrónico corporativo, el fraude por correo electrónico y otras amenazas avanzadas.



Aisla e impide las amenazas multicanal con la integración de Cloudflare Area 1 y el aislamiento remoto del navegador de Cloudflare.



Descubre cuentas y dominios en riesgo, así como dominios nuevos, similares y de proximidad que los atacantes utilicen para omitir SPF/DKIM/DMARC.

Por qué Cloudflare Area 1:



Seguridad preventiva

Identifica la infraestructura del atacante y los mecanismos de entrega con antelación para detener el phishing en las primeras etapas del ciclo de ataque.

Protección integral

Abarca todo el conjunto de tipos de ataque al correo electrónico (URL, cargas útiles, ataques al correo electrónico corporativo), vectores (correo electrónico, web, multicanal) y canales de ataque (externos, internos, socios de confianza).



Análisis contextual

Usa técnicas de detección avanzadas (análisis del lenguaje, visión informática, gráficos sociales, etc.) para detectar ataques contra el correo electrónico corporativo, fraudes al correo electrónico de proveedores y otras amenazas avanzadas.



Protección continua

Implementa una estrategia de seguridad total con capas de protección contra amenazas antes, durante y después de que el correo electrónico llegue a la bandeja de entrada.

Por qué Cloudflare Area 1 y Google Cloud:

- **Mejora de la eficiencia operativa:** reduce la complejidad reemplazando las puertas de enlace de correo electrónico seguras por una arquitectura moderna que prioriza la nube.
- **Implementación flexible y eficaz:** implementa el servicio Area 1, completamente flexible, en menos de 5 minutos e intégralo perfectamente con las funciones nativas de Google Cloud, como la protección contra correo electrónico no deseado, DLP, la encriptación y el archivado.
- **Seguridad SaaS simplificada:** además de la seguridad integrada del correo electrónico en la nube de Area 1, la plataforma Cloudflare Zero Trust proporciona las funciones del agente de seguridad de acceso a la nube (CASB) para Google. Impide fácilmente las fugas de datos y el incumplimiento de la normativa, y utiliza un único servicio integral para acabar con la pérdida de datos, el phishing, el ransomware, Shadow IT y el movimiento lateral en toda la organización.

Caso práctico: empresa de productos envasados de la lista S&P 100 protege a sus ejecutivos y usuarios contra las amenazas del correo electrónico en la nube

Desafíos del cliente	Resultados con Cloudflare Area 1
• Amenazas que sortean Google Workspace y la infraestructura de seguridad existente • Los ataques al correo electrónico corporativo tienen como objetivo a los ejecutivos senior y a los miembros de la junta • Equipo informático que dedica tiempo y recursos constantes a ajustar las reglas de seguridad del correo electrónico y las listas de bloqueo	• +8 millones de ataques dirigidos bloqueados en un año • El equipo informático ahora puede proporcionar mejores métricas e informes de la seguridad del correo electrónico para las reuniones de la junta • Mejoras de la productividad y reducción considerable del riesgo de ciberseguridad

Para descubrir cómo Cloudflare Area 1 puede mejorar tu protección contra el phishing en Gmail, solicita una evaluación personalizada del riesgo aquí.